UNIVERSIDAD JOSÉ CARLOS MARIÁTEGUI

VICERRECTORADO DE INVESTIGACIÓN

ESCUELA DE POSGRADO

MAESTRÍA EN INGENIERÍA DE SISTEMAS E INFORMÁTICA

TESIS

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y CALIDAD DEL SERVICIO DEL COLEGIO CARLOS A. VELÁSQUEZ ILO

PRESENTADO POR

ING. VICTOR HUGO MARTINEZ CAMARA

ASESOR

MG. HUGO EULER TITO CHURA

PARA OPTAR GRADO ACADÉMICO DE MAESTRO EN INGENIERÍA DE SISTEMAS E INFORMÁTICA CON MENCIÓN EN SEGURIDAD Y AUDITORÍA INFORMÁTICA

MOQUEGUA-PERÚ

2023

ÍNDICE DE CONTENIDO

Índice de tablas

Índice de figuras

RESUMEN

El enfoque primordial fue de proponer un sistema de gestión de la seguridad de la información aplicando la normativa ISO 27001 para el colegio Carlos A. Velásquez Ilo, cuyo fin sera minimizar los posibles riesgos en cuanto a perdidas de la información. Fue diseñado cuantitativamente bajo el diseño descriptivo de transcripción no experimental. Así mismo, los resultados fueron plasmados mediante graficas con sus interpretaciones para una mejor comprensión. La población constituida del colegio Carlos A. Velásquez fue de 42 miembros por lo que se usó el total de la población, f ueron encuestados para conocer sus puntos de vista sobre la gestión de la seguridad de la información. Para lograr resultados, los entrevistados enfatizaron la importancia de solicitar propuestas de sistemas de información utilizando la norma ISO 27001. La propuesta cubre los tres factores del sistema de gestión de seguridad de la información relacionados con la norma ISO/IEC 27001 para proteger toda la información solicitada por el Colegio Carlos A. Velásquez Ilo: confidencialidad, integridad y disponibilidad. Por lo tanto, se puede concluir que la propuesta mejorará significativamente el proceso.

Palabra Clave: Gestión de seguridad de la información, ISO 27001, Calidad de servicio.

ABSTRACT

The main focus of this research was to propose an information security management system applying the ISO 27001 standard for the Carlos A. Velásquez Ilo school, whose purpose is to minimize the possible risks in terms of information loss. It was designed quantitatively under the descriptive design of non-experimental transcription. Likewise, the results were captured through graphs with their interpretations for a better understanding. The constituted population of the Carlos A. Velásquez school was 42 members, so the total population was used, who were given a survey to find out their points of view regarding information security management. In order to obtain the results, it was shown that the respondents emphasized that it is important to request the proposal of an information system applying the ISO 27001 standards. This proposal covers an information security management system in accordance with the ISO/ IEC 27001 to maintain three factors, confidentiality, integrity and availability of all the information required at the Carlos A. Velásquez Ilo school. Therefore, it can be concluded that this proposal will significantly improve the processes.

Keywords: Information security management, ISO 27001, Quality of service.

INTRODUCCIÓN

Si nos enfocamos hace quince años, el parte evolutivo tecnológico es y sigue siendo el más grande de nuestra era, con una rápida y creciente evolución de la informática, la estructura de las computadoras y sus conexiones en la red han permitido como la persona percibe de manera distinta nuestro mundo. En el entorno actual, una de las mayores ventajas que tiene un equipo de cómputo en red e internet es la gran cantidad disponible de información, que está literalmente al alcance de todos. Por lo que es muy importante conocer cómo almacenar y resguardar la información de todas las posibles incidencias que pudieran surgir. En una organización, salvaguardar la información es crucial y responsabilidad exclusiva del área encargada. Por lo tanto, el fin primordial de esta investigación es añadir nuevos mecanismos de seguridad que permitan mejorar el rendimiento de la entidad en lo que conlleva a la integridad, exposición, disponibilidad y confidencialidad de la información, Así mismo todo lo que respecta en base a seguridad de la información de los trabajadores del colegio Carlos A. Velásquez Ilo. En el presente capítulo I. Nuestro problema de investigación, se describirá el entorno actual de nuestra problemática relacionado al tema de investigación, basados a través de la observación, percepción con hechos reales y documentales que enfocan su estudio. En la definición del problema se manifestará el tema que se tiene como elemento visualizar, Luego se procederá a reconocer el objetivo de nuestra investigación, la justificación planteada e importancia de dicha investigación, como también se delimitará las variables e hipótesis. En el presente capitulo II. Marco teórico, se desarrollará el análisis de los antecedentes de la investigación tanto internacional como nacional, los precedentes de las bases teóricas para un correcto encaje en el

problema de investigación, así mismo en el marco conceptual que hará alusión a una recopilación de conceptos importantes para el desarrollo del trabajo de investigación. En el presente capitulo III. Método, se realizará una descripción del tipo de investigación, así como del diseño de la investigación, se identificará tanto a la población que conforman y la muestra, así como de indicar las técnicas, los instrumentos y fichas informativas, luego se procederá a enseñar sobre la técnica que se empleará para el procesamiento que se realizó y el análisis de datos que se tomará. En el presente capitulo IV. Se enfocará en la presentación y el objetivo del análisis de los resultados, se efectuará la exposición correspondiente de los resultados que se tendrá por cada variable y se manifestará los resultados. En el presente capitulo V. Presentaremos las Conclusiones y las presentes recomendaciones, Se desarrollará cada conclusión en base a cada hipótesis y resultado, así mismo se desarrollará las recomendaciones que ayudarán en gran medida a la investigación.

CAPÍTULO I

EL PROBLEMA DE INVESTIGACIÓN

1.1. Descripción de la realidad Problemática.

Cualquier sistema de redes de computadoras, tanto nuestro hardware como nuestro software son vulnerables ante una diversidad de factores que pueden ser causados por riesgos humanos y riesgos de índole físicos, los cuales pueden ser fuentes de un sin fin de problemas. Entonces, si partimos de que nuestros sistemas están expuestos a una diversidad de eventos externos como internos, tenemos que tomar acciones ante este problema, marcando decisiones y estrategias lo más precisos posible, por ejemplo: ¿Qué componente de nuestro hardware está fallando?, ¿la información que se ha perdido proviene de un dato o algún archivo, cuando se habría producido y que tan rápido fue la capacidad de respuesta? Estas incidencias nos sirven como ayuda para poder enfocarnos en nuestras estrategias y planes para llevar nuestra seguridad de información.

Ante una eventualidad inesperada, las pérdidas de información pueden ser catastróficas ya sea por algún componente crucial como el disco duro del computador, sabotajes, terremotos, incendios, mal empleo de los sistemas, virus, etc., que podrían causar daños irreparables, por lo que nos queda la recuperación rápida antes de personal capacitad para reconstruir el sistema de

red existente y el sistema de información. Godoy (2014) plantea que, para proteger su información, debemos garantizar la seguridad de nuestra información y sistemas contra el acceso, divulgación, uso, destrucción y/o destrucción no autorizados. Por tanto, el concepto de seguridad debe estar relacionado con la seguridad, la preparación o la falta de riesgo. Por lo que la seguridad es en otras palabras, un estado que muestra la información o sistema que está relativamente libre de riesgo, daño o peligro.

Moscaiza Moncada, (2018), en su tesis "Diseño de un sistema de gestión de la seguridad de la información (SGSI) para la Cooperativa de Ahorro y Crédito ABC, basado en la norma ISO 27001:2013". Nos plasma como podemos gestionar toda la seguridad de la Información en base a la norma ISO 27001:2013 las cuales poseen diversas apariencias que podrían evidenciar la exigencia de dirigir sus procesos hacia un efectivo sistema de gestión de riesgos, donde se realizara un plan de seguridad acorde y cuya función principal es minimizar los riesgos, protegiendo el valor activo que es la información. Deberíamos saber que daño o peligro, es aquello que podría afectar gravemente el funcionamiento o a los resultados que podrían obtenerse. Así mismo, consideramos que es un conjunto de acciones preventivas de la organización y todo aquel sistema tecnológico que protege y resguarda dicha información. En el Perú hay lineamientos para que puedan ser aplicados literalmente por las organizaciones que lideran y operan en el país según las normas ISO 27001, orientada a gestionar íntegramente la seguridad en lo que respecta a la información, la ISO 27002, que son prácticamente recomendaciones para las buenas prácticas en la gestión de la seguridad de la formación y la ISO 27003,

el cual se enfoca en cómo podemos diseñar e implementar un sistema correcto. Actualmente en el Perú, la mayoría de organizaciones públicas y privadas ya están optando por implementar e innovar un sistema que ayude a complementar la seguridad de la información interna y externa producidas al interior de las mismas.

Actualmente en el colegio Carlos A. Velásquez Ilo, no cuenta con un buen sistema pleno de gestión de seguridad de la información en los servicios informáticos donde la calidad del servicio es mínima, por ello deberían darle énfasis en salvaguardar y proteger todos estos activos de información a través de mecanismos que nos aseguren primeramente la integridad, accesibilidad, confiabilidad y restauración de la información, puesto que nuestros estudiantes, padres de familia, la Ugel Ilo y el mismo Minedu requieren la información que el colegio genera, por tanto el colegio debe tener la capacidad de respuesta y velar a través de su personal de proteger todo lo concerniente a la información existente. Por lo tanto, el fin principal de esta investigación es acondicionar nuevos mecanismos de seguridad que permitan mejorar el rendimiento de la entidad, en todo lo concerniente a la definición, disponibilidad, integridad y confidencialidad del activo cuyo valor es la información, así mismo ver el intelecto específicamente en cuanto a seguridad de la información del personal que labora en el colegio Carlos A. Velásquez Ilo. Cabe recalcar que en el colegio no hay personal dedicado en esa área por lo que si no se soluciona o se da prioridad tendrán perdidas de tiempo en la entrega de información o la información podría ser adulterada. Todo ello me lleva a plantear la siguiente interrogante:

¿El desarrollo o implementación de un sistema de gestión de seguridad de información ayudará al colegio Carlos A. Velásquez Ilo, en evaluar la calidad del servicio?

1.2. Definición del problema

1.2.1. General

¿Entre el SGSI y la calidad del servicio del colegio Carlos A. Velásquez Ilo, cuál sería su correlación?

1.2.2. Específicos

- ¿Cuáles serán los principios de seguridad de la información en correlación a la calidad del Servicio del colegio Carlos A. Velásquez Ilo?
- ¿Cómo el ISO/IEC 27001 se correlaciona con la calidad del servicio del colegio Carlos A. Velásquez Ilo?
- ¿Cómo la administración de seguridad de la información se correlaciona con la calidad del servicio del colegio Carlos A. Velásquez Ilo?
- ¿Cómo el SGSI se correlaciona con la calidad del Servicio del colegio Caros A. Velásquez Ilo?

1.3. Objetivo de la investigación

1.3.1. Objetivo general.

Establecer cuál será la correlación entre un SGSI y la calidad del servicio del colegio Carlos A. Velásquez Ilo.

1.3.2. Objetivos específicos.

- Identificar los principios de seguridad de la información en correlación a la calidad del servicio del colegio Carlos A. Velásquez Ilo.

- Identificar como el ISO/IEC27001 se correlaciona con la calidad del servicio del colegio Carlos A. Velásquez Ilo.
- Identificar la administración de seguridad de la información en correlación con la calidad del servicio del colegio Carlos A. Velásquez Ilo.
- Identificar como el SGSI se correlaciona con la calidad del servicio del Colegio Carlos A. Velásquez Ilo.

1.4. Justificación e importancia de la investigación.

1.4.1 Teórica.

Utilizar la serie ISOS 2700X, el Reglamento Técnico del Perú, el Modelo de Calidad de Servicios Informáticos y otros marcos teóricos como guía de evaluación para evaluar y comprender la relación entre el sistema de gestión de seguridad de la información y la calidad del servicio. Colegio Carlos A. Velásquez Ilo, para garantizar la calidad del servicio, es necesario optimizar y minimizar la ocurrencia de eventos que obstaculicen la confidencialidad, disponibilidad e integridad. Riesgos operativos que puedan sufrir la información o determinados sistemas informáticos del colegio. Se citarán diversos precedentes nacionales e internacionales que abordan y dan seguimiento a esta investigación sobre protección de la información y su relación con la calidad del servicio.

1.4.2. Metodológica.

Paulatinamente se pueden utilizar métodos de investigación y métodos científicos para cuantificar los resultados obtenidos a través de cuestionarios. Los resultados obtenidos se expresarán con gráficos y su interpretación.

1.4.3. Práctica.

La investigación resulta conveniente, debido a que contribuirá con la mejora de un SGSI y su implicancia en la calidad del servicio del colegio Carlos A. Velásquez Ilo, siendo punto de partida de imitar por otros colegios o de nuevo personal encargado de continuar con las mejoras continuas.

Finalmente, el colegio podrá adoptar mejoras en su sistema de gestión de seguridad de la información.

1.5. VARIABLES Y OPERACIONALIZACION

1.5.1 VARIABLE INDEPENDIENTE

Sistema de gestión de seguridad de la información.

1.5.2 VARIABLE DEPENDIENTE

Calidad del servicio del colegio Carlos A. Velásquez Ilo.

1.5.3 Operacionalización Variable Independiente

Tabla 1

Operacionalización variable Independiente

Variable	Definición conceptual	Definición operacional	Dimensiones/Factores	Indicadores	Ítem	Unidad/Categoría	Instrumento	Escala
SGSI	Para la NTP-ISO/IEC 27001;2018, todo SGSI tiene libertad de que los activos de la información se gestionen de forma ordenada, por lo que en la entidad se debe realizar un procedimiento único para minimizar riesgos (p.28)	La ISO 17799, Vendría hacer un grupo de procedimientos, políticas, y directrices, así como recursos y actividades que van asociados colectivamente por una organización, con el fin de salvaguardar sus activos como es la información.	Principios de seguridad de la información. (Estándar, 2005) Norma ISO/IEC 27001. (ISO, 2015) Administración de sistema de gestión de seguridad de la información (Disterer, G., 2013) SGSI (ISO, 2015)	Disponibilidad Confidencialidad Plan Conocimiento Capacitación Existencia de Personal. métodos de divulgación. Sistema de gestión de seguridad Medición de seguridad Personal especializado para amenazas Métodos para respaldar la recuperación de la información Medios de respaldo Comunicación inmediata ante siniestros Políticas de seguridad Gestión de riesgos Auditorías Elaboración documentada Actualización mejoras	1-8 9-11 12-22 23-35	Totalmente en desacuerdo. En desacuerdo. Ni de acuerdo ni en desacuerdo. De acuerdo. Totalmente de acuerdo.	Cuestionario	Ordinal

***Nota*:** Elaboración propia

1.5.4 Operacionalización Variable dependiente

Tabla 2

Operacionalización variable dependiente

Variable	Definición conceptual	Definición operacional	Dimensiones/Factores	Indicadores	Ítem	Unidad/Categoría	Instrumento	Escala
Calidad del servicio del colegio Carlos A. Velásquez Ilo	Según Kotler y Armstrong (2013) para la satisfacción del cliente tiene que haber calidad vinculada a un valor.	Según el autor (Fontalvo, Vergara & de la Hoz, 2012), Enfocado en como el personal dispone de sus servicios la disponibilidad y el interés para atender los distintos requerimientos solicitados mediante sus equipos existentes el orden y la apariencia de sus recursos físicos.	Perceptibles	Identificación	1	1. Totalmente en desacuerdo	Cuestionario	Ordinal
				Apariencia	2			
				Tecnología	3			
			Facultad de solución	Aspecto	4	2. En desacuerdo		
				Profesionalismo	5			
				Tiempos	6			
				Acceso	7			
				Flexibilidad	8	3. Ni de acuerdo ni en desacuerdo		
				eficiente	9			
			Empatía	Disponibilidad	10			
				Respetuoso	11			
				Servicial	12	4. De acuerdo		
			Seguridad	habilidad	13			
				Credibilidad	14			
			Fiabilidad	Oportuno	15	5. Totalmente de acuerdo		
				Confianza	16			

***Nota*:** Elaboración propia

1.6. Hipótesis de la investigación.

1.4.2 Hipótesis general

Si existe una correlación entre el SGSI y la calidad del servicio del colegio Carlos A. Velásquez Ilo

1.4.3 Hipótesis especificas

- Los principios de seguridad de la información; se correlacionan en gran medida con la calidad del servicio del colegio Carlos A. Velásquez Ilo.
- El ISO/IEC 27001; se correlaciona en gran medida con la calidad del servicio de colegio Carlos A. Velásquez Ilo.
- La administración de seguridad de la información; se correlaciona en gran medida con la calidad del servicio del colegio Carlos A. Velásquez Ilo.
- El SGSI; se correlaciona en gran medida con la calidad del servicio del colegio Carlos A. Velásquez Ilo.

CAPÍTULO II

MARCO TEÓRICO

2.1 Antecedentes de la investigación

2.1.1 Antecedentes a nivel Internacional.

- Carlos Mero Suárez, 2018, cuyo diseño fue "Plan de contingencias informáticas y la seguridad de la información en el consejo nacional electoral de la provincia de santa elena", Su principal objetivo es preservar la integridad de la Comisión Nacional Electoral del Departamento de Santa Elena en relación con este presunto incidente informático, haciendo un estudio previo para determinar la metodología, en qué etapa esta la seguridad, si tiene políticas de privacidad, si es confiable y si la información que manejan es integra.
- Héctor Acosta Ramírez, 2017, el cual elaboró un "Diseño de un plan de contingencia del sistema de información para la entidad ITRC", donde nos habla de un plan de contingencia que se preste a dar respuesta inmediata a los sucesos que pudiesen ocurrir, habilitando y restableciendo prioritariamente los servicios esenciales informáticos en un tiempo prudente establecido por su centro de trabajo.

Su trabajo de investigación fue enfocado dentro de lo posible en un proyecto de investigación factible. Donde tomó la muestra a 10 trabajadores del área de Tecnologías de la agencia ITRC. El método de recopilación de información es una revisión de documentos, examinando aquellos que ya son relevantes para la gestión de seguridad de la información, tales como: ISO/IEC 27001, ISO/IEC 27002 e ISO/IEC 27005.

- Katherine Ladines Garcés, 2017, el cual ha denominado su trabajo "Plan informático de contingencia para la seguridad de la información del departamento TIC de la Pucese". Este proyecto de investigación recomienda el desarrollo de un plan de emergencia debido a los riesgos extremos que existen en la ciudad de Esmeralda, donde los movimientos sísmicos son el principal riesgo.

  Es un proyecto que es factible, el cual se tomó a 8 trabajadores del departamento de TIC de la zona PUCESE como población. La técnica utilizada fue la encuesta, para las entrevistas se desarrollaron cuestionarios.

- Calderón Vicente Gonzalo, 2017, donde su título es "Plan de contingencia para el departamento de sistemas de la empresa Ramon & Romero computadoras y suministros de la ciudad de Quevedo", en dicho proyecto de investigación para detectar y prevenir vulnerabilidades en la infraestructura de red estructurada, es que realizan el diseño robusto de un plan de contingencia enfocado a la informática con el único fin de una vez detectado corregirlo en el momento idóneo y así los riesgos se van minimizando.

El método que utilizaron fue cualitativo y cuantitativo, y para la recolección de datos utilizaron encuestas, la herramienta fue un cuestionario para usuarios de la empresa.

- José Verdú Fernández, 2015, cuyo trabajo de investigación "Plan de contingencias de tecnologías de la información en entornos distribuidos", donde nos muestra los fundamentos de lo que es un plan de contingencia, su importancia y porque es importante su elaboración, en dicho trabajo se enfocó en el proyecto TI donde el plan ya existente analizarlo y mejorarlo para la entidad bancaria nacional que tiene en su cartera aproximadamente más de 14 millones de clientes. Dicha mejora es automatizar las acciones, reduciendo sustancialmente la mano del hombre tanto de obra como especializada, administrando los recursos al máximo sin bajar su rendimiento.

2.1.2 Antecedentes a nivel Nacional.

- Omar Israel Moscaiza Moncada, (2018), "Diseño de un sistema de gestión de la seguridad de la información (SGSI) para la Cooperativa de Ahorro y Crédito ABC, basado en la norma ISO 27001:2013". Muestra cómo gestionar la seguridad de la información según la norma ISO 27001:2013, que tiene muchos matices, y muestra claramente la necesidad de avanzar sus procesos hacia un sistema de gestión de riesgos eficaz., donde se realizara un plan de seguridad acorde y cuya función principal es minimizar los riesgos, protegiendo el valor activo que es la información.

- Bach. Yan carranza, freddy Bach. Zavala Vásquez, Cinthia (2018). En su tesis: “Plan para perfeccionar el grado de estabilidad de reportes y seguida del centro de datos en la gerencia regional de Educación de la Libertad aplicando cada uno de los pasos ISO 27001 y buenas prácticas COBIT”, Se basa principalmente en una propuesta de programa para mejorar la seguridad informática en los centros de datos de gestión regional a través de auditorías del sistema MAIGTI basadas en la norma ISO 27001 y diversos lineamientos del sistema. COBIT 4.0. Determinándose también que procesos son los más adecuados para el control según los estándares las evaluaciones necesarias y recomendaciones necesarias.
- Gonzales Sosa, Henry Jesús, 2018, cuyo proyecto se denomina “diseño del plan de contingencia como herramienta para gestionar riesgos de la seguridad de la información en el área del centro de sistemas de información de la ugel-ferreñafe en el periodo 2018”, en su investigación optan por realizar un plan de contingencia exclusivamente para el centro de sistemas de información de la Ugel Ferreñafe, siendo sus variables como la independiente el plan de contingencia y en cuanto a la variable dependiente la gestión de riesgos. Dado que se enfocan en conceptualizar todo lo concerniente a la elaboración del plan, es que hacen una encuesta para saber la real situación de la ugel, su enfoque fue descriptivo y explicativo.
- Vergara Quiroz, Gladis, 2016, cuyo proyecto denominado es “Seguridad de información y calidad de servicio en la Universidad Nacional Federico Villarreal, 2016”, Nos muestra la relación entre seguridad de la información y calidad del servicio en esta universidad, su investigación es de tipo básico,

en este proyecto se eligió el nivel de descripción no experimental adecuado, su corte transversal es transversal, su población es 55 usuarios, el método que utilizaron. Utilizando el enfoque hipotético-deductivo, su enfoque fue cualitativo y cuantitativo y utilizaron SPSS para gestionar todos los datos.

- Javier Seclén Arana, 2016, cuyo plan de tesis fue "Factores que afectan la implementación del sistema de gestión de seguridad de la información en las entidades públicas peruanas de acuerdo a la NTP-ISO/IEC 27001", Describe en detalle cómo identificar potenciales factores de influencia cuando dichos sistemas son implementados en las instituciones públicas peruanas, con el objetivo principal de analizar las limitaciones y desafíos que enfrentan los sistemas de gestión de seguridad de la información de las instituciones públicas. Su método de investigación es de nivel descriptivo no experimental y transversal, utilizando entrevistas para obtener información y datos que puedan ayudar a mejorar el desarrollo de estándares de seguridad de la información según NTP-ISO/IEC 27001, revelando ocho posibles categorías de impacto. Implementación de sistemas de gestión de sistemas de información en las instituciones públicas del estado peruano.

2.2 BASES TEÓRICAS

2.2.1 Definición de seguridad de la información

Si hablamos de seguridad de la información utilizando la norma ISO 2700, se basa en todos los procedimientos necesarios para proteger la información, mantenimiento, prevención, centrándose en la confidencialidad, asegurando que la información esté completa y disponible ante cualquier riesgo que pueda surgir. Destruirlo desde fuera o desde dentro (Quinde, 2014).

Lo que representa la seguridad en sí, trae de la mano una falta de amenazas, por lo que en este mundo globalizado es muy difícil de sostener, todas las sociedades que existen actualmente son de riesgo, y este riesgo será siempre permanente en todos las sociedades y estados, en este sentido la seguridad no es una ausencia en sí de amenazas. (Barrantes Porras & Hugo Herrera, 2012).

La Real Academia Española, manifiesta que seguridad es sinónimo de seguro y seguro es tener todo bajo control exento de innumerables riesgos que pudieran ocurrir.

(Asociación Española para la Calidad, 2018), La seguridad de la información tiene como objetivo proteger la información y todo lo relacionado con los sistemas de información, el control de acceso, su uso, la confidencialidad, otras intromisiones o destrucción, incluso con todos los métodos posibles todavía hay un margen debido a la vulnerabilidad Nada es absolutamente Seguro, cuando se trata de sexo, y los riesgos siempre son posibles. Con base en la definición anterior, podemos definir la seguridad de la información como el monitoreo y protección de los datos de la información de agentes externos e internos para reducir sus riesgos.

2.2.2 Definición de informática

El ser humano siempre ha tratado de automatizar los procesos manuales en digitales, agilizando procesos, realizando los trabajos cada vez más rápidos y simplificando procesos innecesarios, así mismo la aparición de máquinas son una gran ayuda al hombre, siendo más rápidos y eficientes. (Erb, 2005).

Se basa en proteger la información alojada de un computador o a través de redes, así como su infraestructura, a través de normas, métodos, procedimientos cuyo objetivo es mantener seguro y confiable un sistema de información (Arroyo Fuentes, 2016).

La Real Academia Española, manifiesta que la palabra informática es un conjunto de varios conocimientos de índole científicos que emplean técnicas para automatizar el proceso de la información a través de ordenadores.

2.2.3 Objetivo de la Seguridad Informática.

(Gómez A, 2011) Entre los principales son:

- Los riesgos que pudieran existir se tendrían que reducirlos y gestionarlos, así detectaríamos y preveríamos problemas y amenazas futuras en cuanto a seguridad.
- Administre eficientemente los recursos y la cantidad de aplicaciones del sistema..
- Reducir las pérdidas y responder eficientemente ante un problema asociado con la seguridad.
- Cumplir con los contratos en los marcos legales establecidos con los clientes

2.2.4 Importancia de la Seguridad Informática.

(García A, Hurtado C, Alegre M, 2011). Tenemos que tener en cuenta que para evitar pérdidas económicas y tiempo en una empresa y/o organización, debemos mantener la información y la integridad del sistema informático, sin olvidar el riesgo que puede ocasionar el acceso ajeno de usuarios no autorizados que entren al sistema. Así mismo manifiestan que encontramos

elementos y métodos que podrían ser de hardware y software, aparatos físicos y recursos humanos los siguientes:

- Comprender las razones y/o fundamentos de la seguridad informática y el rol crucial de mantener y prever un sistema seguro.
- Tenemos que tener conocimientos básicos y diferenciar correctamente las distintas clases de seguridad que hay actualmente.
- Conocer a que apunta la seguridad, cual es el objetivo.
- Saber y poder distinguir tipos de amenazas existentes.
- Tener como prioridad el de salvaguardar físicamente los sistemas informáticos así mismo ver las condiciones ambientales existentes.
- Tener conocimiento sobre las leyes y normas enfocadas a todo lo que es seguridad informática.

2.2.5 Vulnerabilidades.

(Areitio J, 2008) Si hablamos de vulnerabilidad, no es dañina en sí misma; Es solo una o más condiciones donde cabe la posibilidad que una amenaza logre afectar al activo. Estas vulnerabilidades pueden ser permanentes si el activo es tal que los cambios en el activo no afectan la vulnerabilidad. Las vulnerabilidades suelen ser debilidades o defectos donde un intruso puede aprovechar y dar consecuencias no deseables.

2.2.6 Amenazas

(Gómez A, 2011) Las amenazas pueden causar daños en los sistemas informáticos causando pérdidas de diferente índole ya sea intencionado o por algún accidente en la organización. Dichas amenazas pueden clasificarse en:

- Amenazas por casusas naturales.
- Amenazas por causas de Agentes Externos.
- Amenazas por causas de Agentes Internos.

(Corrales, 2005) Pueden existir cuatro categorías que pueden afectar la seguridad de un sistema informático:

- **Interrupción**: Es cuando en el sistema se destruye algún recurso o no está disponible, dicha agresión de disponibilidad es grave. Ejemplos: disco duro roto, o las líneas de comunicación están rotas.
- **Intercepción:** Cuando un sujeto, programa o un ordenador ajeno al sistema, accede a cualquier recurso del sistema, por lo que se denomina agresión de confidencialidad.
- **Modificación**: Cuando una persona ajena al sistema, además de acceder al recurso lo modifica, por lo que se denomina agresión de integridad. Ejemplo: cuando un programa no funciona como debe ser, dando información errada.
- **Fabricación**: Cuando un recurso fue adulterado por alguien no autorizado e inserta en el sistema objetos falsos, por lo que se denomina agresión de autenticidad.

2.2.7 Riesgos

(Aguilera P, 2010). Es la posibilidad de que una amenaza aparezca a raíz de una vulnerabilidad. Si no hay amenazas no hay riesgos. Así mismo ante un riesgo pueden optarse por tres alternativas:

- Cuando se asume riesgo, pero el operario lo ignora.
- Transferido.

- Para anular o reducir el riesgo se aplican medidas.

(Areitio J, 2008), en su libro argumenta que “Hay tres factores de riesgo principales en la seguridad de la información.”, estos son:

- Ambientales/Físicos:
- Tecnológicos
- Humanos.

2.2.8 Norma ISO 17799

Myler & Broadbent (2006) se centra en los responsables de implementar, mantener e iniciar la gestión de seguridad de la información de manera efectiva y eficiente utilizando estándares internacionales al implementar esta gestión en las organizaciones. Enfatice que esta información es un activo valioso para cualquier organización o negocio. Las empresas que implementan un sistema de gestión de la información según la norma ISO 17799 han demostrado tener los siguientes beneficios:

- Mejoramiento eficiente en la administración y adecuado plan en la seguridad de la información.
- Protecciones adicionales de los sistemas de información.
- Para la continuidad operacional del negocio establece garantías.
- Mejor ordenamiento para los procesos de auditoría interna.
- Usuarios tendrían mayor confianza en el uso de aplicaciones.
- La organización tendrá un valor comercial e imagen

2.2.9 Norma ISO/IEC 27001

(Disterer, 2013), Basándose en gestionar los adecuados controles para el riesgo operacional, que se basan en niveles de aceptación los cuales son tomados como base.

2.2.10 Modelo SERVQUAL

Scardina (1994). Zeithaml, Parasuraman, Berry generaron la calidad del servicio, El objetivo es mejorar, simplificar y gestionar diversas perspectivas para mejorar la calidad de los servicios prestados por la empresa. Esta medición requiere un cuestionario para evaluar y verificar características que cubren las cinco dimensiones propuestas: aspectos protectores, confiabilidad, capacidad de respuesta, empatía y tangibles. La conclusión es que los modelos de escala de respuesta múltiple están diseñados principalmente para comprender diferentes perspectivas de los usuarios o clientes sobre los servicios. Por tanto, estas necesidades de los clientes son medidas por SERVQUAL para una empresa de servicios que se posiciona en una de las cinco dimensiones mencionadas por Scardina (1994).

2.2.11 Norma ISO 9001 orientado a los servicios

Según Juran (1989), para poder satisfacer las perspectivas y requerimientos de los usuarios es que se emplea la ISO 9001 que es un grupo de rasgos hereditarios de un servicio y/o bien.

Para Deming (1986), la calidad debe garantizar la satisfacción del cliente, el cual requieren de propiedades adecuadas, las cuales se mencionarán según la ISO 9001:

- Un rol importante para el cliente es el proceso de apoyo para el servicio.
- Ya no es posible ser corregido Una vez que el servicio es prestado.
- En una empresa los servicios son intangibles.
- El servicio es directo con el usuario.
- Difícilmente se puede estandarizar el servicio al usuario y/o cliente.
- Se personaliza el servicio contratado que necesitan los clientes, determinando su grado de satisfacción.
- Para cubrir las necesidades del cliente se deben determinar responsabilidades.

2.2.12 Servicios de Seguridad de la Información

(Gómez A, 2011) Durante los procesos de seguridad informática hay que estipular los siguientes servicios:

- **Confidencialidad.**

  Este servicio garantiza que la información transmitida o alojada, solo podrá ser visto por su destinario perfectamente acreditado.

- **Autenticación.**

  En este servicio garantiza que el mensaje enviado por su creador es legítimo y el destinatario podrá estar seguro al recibir dicho mensaje.

- **Integridad**

  Este servicio garantiza que el mensaje creado no ha sido adulterado a través de la red.

- **No Repudiación.**

Este servicio a través de un mecanismo pretende demostrar quien ha enviado el mensaje para que luego no pueda negarse, demostrando la autoría y envió del mismo, al igual que aplicaría para el destinario.

- **Disponibilidad.**

  Ante la ola de ataques e intromisiones se pretende diseñar un sistema robusto para que funcione correctamente, y estar disponible permanentemente para que puedan acceder los usuarios.

2.2.13 Consecuencias de la Falta de Seguridad

(Gómez A, 2011) Las falencias en las vulnerabilidades de los sistemas informáticos que hoy en día se manejan, pueden ocasionar perdidas principalmente económicas, sobrepasando por encima las perdidas por medios de robos o ingresos no autorizados en algunas de las instalaciones. Por lo tanto, es importante proteger los datos de la información.

2.2.14 Políticas de Seguridad

(Aguilera P, 2010) Las políticas de seguridad pertenece en su conjunto a la política general, es por ello que en una empresa u organización tienen que ser aprobados por la dirección ya que el objetivo de dichas políticas es concientizar a todo el personal y a los mismos encargos de los sistemas de información, de conocer los principios que establecen la seguridad en dicha empresa y normas enfocadas para alcanzar los objetivos. Dichas Políticas no pueden ser iguales, son de acorde a la realidad de cada organización.

2.2.15 Objetivos de las Políticas de Seguridad.

(Aguilera P, 2010) Enfocados en cinco grupos:

- Identificar los riesgos, necesidades y evaluación ante las consecuencias de posteriores ataques.
- Para implementar medidas de seguridad es necesario considerar qué medidas de seguridad son adecuadas para prevenir los riesgos que plantean los activos de información.
- Proporcionar los procedimientos y las reglas generales que se deben aplicar para evaluar y afrontar los riesgos que se han identificado en cada organización.
- Detectar ante un análisis minucioso de los sistemas de información y las aplicaciones instaladas, las vulnerabilidades existentes para así controlarlos las amenazas y fallos que los activos producen.
- Establecer un plan de contingencia.

2.2.16 Plan de respuesta a incidentes

(Terán D, 2014) Dicho plan puede ser dividido en cuatro etapas:

- Investigar el Incidente.
- Acción oportuna e inmediata para minimizar o frenar el incidente.
- Reporte de incidentes.
- Restauración de los servicios o recursos que fueron afectados.

Por lo que tiene que ejecutarse en el momento, los tiempos son cruciales, es por ello que deben de organizarse para efectuar capacitaciones y practicas ante incidentes para medir los tiempos de respuesta minimizando o reduciendo el impacto.

2.2.17 Detección y oportuna respuesta ante incidentes que afectan la seguridad.

(Chicano E, 2014) Permite a las organizaciones la automatización de números procesos de respuestas ante incidentes y la reducción considerable de los daños ocasionados, a la vez que se facilita la recuperación de los sistemas afectados. Además de la confección del Plan propuesto de Gestión de Incidentes, deberá encargarse de establecer:

- La política general de gestión de incidentes en la que debe basarse el plan de gestión.
- Procedimientos basados en política e incluidos en el plan.
- Relación entre el equipo de respuesta a incidentes y otros equipos internos y externos a la organización.
- Instrucciones que definen los procedimientos que debe seguir la organización en la comunicación con terceros en caso de incidencia.
- Organización del personal responsable de la gestión de respuesta a incidentes e identificación y asignación de funciones.

2.2.18 Plan de contingencia

(Aguilera P, 2010) Es un instrumento elaborado por personal calificado, que contiene todas las medidas y procedimientos que garantice la continuidad de la entidad, donde protege y recuperar los sistemas ante amenazas e impactos. Consta de tres subplanes:

- **Plan de Respaldo. -** Medidas preventivas antes que se sufra un daño. por ejemplo, para restaurar los sistemas usando las copias de seguridad previamente creados o ante una eventualidad como incendio se activa el sistema de manera automática.

- **Plan de Emergencia**. - Cuando el sistema este siendo atacado, que medidas se deben tomar en el momento del incidente.
- **Plan de Recuperación**. - Una vez producido el desastre, es evaluar y volver el sistema al estado normal operativo. Ejemplo, reinstalar las distintas aplicaciones, reemplazar los equipos o materiales afectados y las copias de seguridad creadas previamente tratarlas de restaurarlas.

2.2.19 Plan de Emergencias

(Corrales, J, 2005). Es una guía donde se alojan los procedimientos necesarios durante o después de cada daños o error. Determinándose las siguientes acciones:

Acciones inmediatas:

- En la seguridad Física: llamar a los encargados, dar aviso para activar o desactivar alarmas que se tengan, el empleo correcto de los extintores.
- En la seguridad Lógica: es donde se tiene que llamar al jefe encargado del área, velar por salvaguardar el computador central, comunicaciones y/o periféricos.

Acciones posteriores:

- En la seguridad Física: que acciones tomar, análisis de daños, y el respectivo informe.
- En la seguridad Lógica: volver a activar el sistema operativo, los procesos, analizar los daños que han causado, emplear las copias de seguridad alternativos.
- Designación de Responsabilidades: delegación de funciones.

2.2.20 Backups

(Corrales, J, 2005) Ante las posibles fallas de los sistemas tanto de la parte física como lógica, incidencias naturales y demás, se debería tomar acciones apropiadas para tratar y frenar los daños, por ello el objetivo es la planificación y procedimientos apropiados como las copias de seguridad, backups, entre otros.

Según lo dicho por el Institute of Electrical and Electronics Engineers, las casuales pueden ser conformados por las siguientes categorías:

- Físicos: fallos tanto de hardware, de medio o fallo de CPU.
- Errores de software: fallos de los programas instalados.
- De operación: Configuraciones inadecuadas, inexperiencia de los encargados de la información o procedimientos incorrectos de Backups.

2.3 MARCO CONCEPTUAL

La conceptualización de términos que es muy importante para entender el desarrollo del trabajo de investigación.

- **Autenticidad:** se valida la información del emisor para evitar posibles suplantaciones. (ISO/IEC, 2014).
- **Calidad del servicio:** basado en cumplir la satisfacción y expectativas del cliente a través de un servicio que logre llenar sus necesidades. (Molina, 2014).
- **Confidencialidad:** Las personas autorizadas para acceder el sistema tienen la garantía que la información manejada es la correcta y solo son para ellas. (ISO/IEC, 2014).

- **Disponibilidad:** que la información y demás recursos solo puedan ingresar los usuarios autorizados y que estén disponibles permanentemente (ISO/IEC, 2014).
- **Integridad:** Donde la información total y el procesamiento son íntegros. (ISO/IEC, 2014).
- **No repudio:** evitar que la información enviada sea negada por terceros. (ISO/IEC, 2014).
- **Plan de seguridad:** Permitan ejecutar y realizar las decisiones para la correcta gestión de riesgos. (ISO/IEC, 2014).
- **Política de seguridad**: Se debe establecer un conjunto específico de reglas y procedimientos para proteger los activos de información. (ISO/CEI, 2014).
- **Seguridad de la información:** Ante los accidentes o acciones de personal ajeno que pueden dañar los activos de información, nos plasma la capacidad de aguantar con cierto nivel de confianza. (ISO/IEC, 2000).
- **SGSI:** Del tipo marco de trabajo de acuerdo a las normas internacionales para los SGSI. (ISO/IEC 27000:2016, 2016).

CAPÍTULO III

MÉTODO

3.1 Tipo de investigación

Esta investigación se basa en el tipo descriptivo – correlacional.

(Rodríguez, Gil, & García, 1996) y (Bernal, 2013) en sus manifestaciones sobre la metodología que conlleva a la investigación de enfoque cualitativa y enfoque cuantitativo, nos enseña diversos tipos que se empleará en esta investigación:

a) Describir, medir y evaluar aspectos y dimensiones del fenómeno en estudio para describir cómo se formula la pregunta de investigación. Esto nos proporciona información para realizar más investigaciones y desarrollar estrategias de respuesta adecuadas.
b) Correlación ya que mide el grado de asociación/correlación entre dos componentes o variables en estudio.

3.2 Diseño de la investigación.

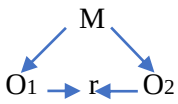
No experimental, las variables no se variarán intencionalmente y de corte transversal/transeccional porque se efectuará en un único momento (Hernández, 2014):

a) Diseño no experimental porque n

b) o se manipulan los elementos causales para determinar sus efectos. Describir y ser capaz de estudiar la aparición de variables a lo largo del tiempo o, en su defecto, las relaciones entre variables.

c) Transversal, incluyendo el nivel descriptivo-correlacional para su estudio.

A continuación, se presenta el esquema correlacional:



Donde:
M = Es la muestra
O_1= La Observación de la V.1
O_2= La Observación de la V.1
r= La Correlación entre dichas variables

3.3 Población y muestra.

3.3.1 Población

La población está conformada por 42 miembros del colegio Carlos A. Velásquez los cuales se describen a continuación.

Tabla 3

Personal docente administrativo de la I.E. Carlos A. Velásquez

N°	PERSONAL	CANTIDAD
1	Director	1
2	Coordinadores	5
3	Personal administrativo	8
4	Docentes de computo	2
5	Docente de DAIP	1
6	Docentes nombres y contratados	25
	TOTAL	**42**

Nota: Datos tomados de secretaria del colegio Carlos A. Velásquez (2023)

3.3.2 Muestra

(López, 2004), se enfoca muestra a una parte de la población en donde se estudiará y ayudará a simbolizar yo representar.

(Castro, 2003), indica que, si la población considerada es menor de 50 personas, la población corresponderá a la muestra. En este estudio usaremos la población total porque la población total es menos de 50, por lo que no necesitamos hacer un muestreo.

3.4 Técnicas e instrumentos de recolección de datos

3.4.1 Técnicas.

(Torres & Paz, 2006), Los métodos de recolección de datos se refieren a actividades que permiten obtener información y con ello alcanzar objetivos, para ello se utilizara la encuesta que se elaborará con preguntas para marcar Si/No, elegir algunas de las opciones, etc. o preguntas abiertas para que responda con sus propias palabras.

El autor (Campoy & Gómez, 2015), menciona que la encuesta es un procedimiento científico de almacenamiento de datos el cual permite obtener información del objeto en estudio.

3.4.2 Instrumentos.

Nuestro instrumento para esta investigación fue el cuestionario para la recolección de datos a procesar.

Para el INEI (2006, P.15), la herramienta que más acogida tiene para recabar datos es el "cuestionario", el cual se compone básicamente de preguntas en relación a sus variables que puede ser una a más; en dichas respuestas se obtendrán los datos para su proceso para ver las singularidades de la población tomada, generalmente este instrumento del cuestionario es el que nos permite alcanzar el propósito de nuestro estudio.

3.5 TÉCNICAS DE PROCESAMIENTO Y ANÁLISIS DE DATOS

Para el tratamiento de los datos, se utilizó el aplicativo SPSS v 24 y Excel.

Para la clasificación y ordenamiento de los datos se utilizó tablas con las frecuencias generadas y gráficos para plasmar lo estadístico.

Se utilizará la estadística Rho de Spearman para comparar hipótesis generales y específicas.

Cuadro informativo

a) SGSI

- Técnica: Encuesta
- Instrumentos: Cuestionario
- Tipo de escala: Ordinal
- Fiabilidad: Coeficiente de Alfa de Cronbach
- Alcance: Colegio Carlos A. Velásquez
- Forma de administración: Encuesta directa

b) Calidad del servicio.

- Técnica: Encuesta
- Instrumentos: Cuestionario
- Tipo de escala: Ordinal
- Fiabilidad: Coeficiente de Alfa de Cronbach
- Alcance: Colegio Carlos A. Velásquez
- Forma de administración: Encuesta directa

CAPÍTULO IV:

PRESENTACIÓN Y ANÁLISIS DE LOS RESULTADOS

4.1. Presentación de resultados por variables.

Utilizamos un cuestionario para obtener datos sobre los sistemas de gestión de seguridad de la información y variables de calidad del servicio de 42 docentes administradores de la Escuela Carlos A. Velásquez Ilo. Luego fueron procesados en Microsoft Excel e IBM SPSS Statistics 29.

4.1.1. Explicación estadística de la variable sistema de gestión de seguridad de la información.

A) MAGNITUD 1: Principios de seguridad de la información

Tabla 4

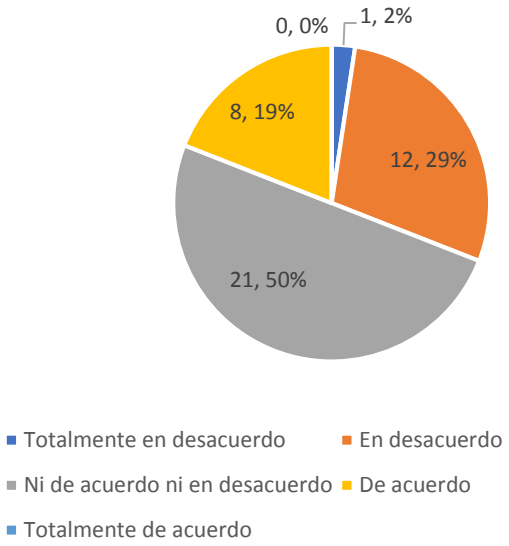
Cuadro de periodicidad de la magnitud principios de seguridad de la información.

Categorías	Frecuencia	Porcentaje (%)	Porcentaje acumulado
Totalmente en desacuerdo	1	2.38%	2.4%
En desacuerdo	12	28.57%	31.0%
Ni de acuerdo ni en desacuerdo	21	50.00%	81.0%
De acuerdo	8	19.05%	100.0%
Totalmente de acuerdo	0	0.00%	
Total	42	100%	

Nota: Dicho esquema es elaboración de mi autoría.

Figura 1

Ilustración de la magnitud principios de seguridad de la información



Nota: La presente representación es elaboración de mi autoría.

Interpretación: Como se puede visualizar en el cuadro 4 y en la representación 1, en lo que respecta a preguntas relacionadas a la magnitud de los principios de seguridad de la información está dominada por la categoría "ni de acuerdo ni en desacuerdo", que representa el 50%

B) MAGNITUD 2: ISO/IEC 27001

Tabla 5

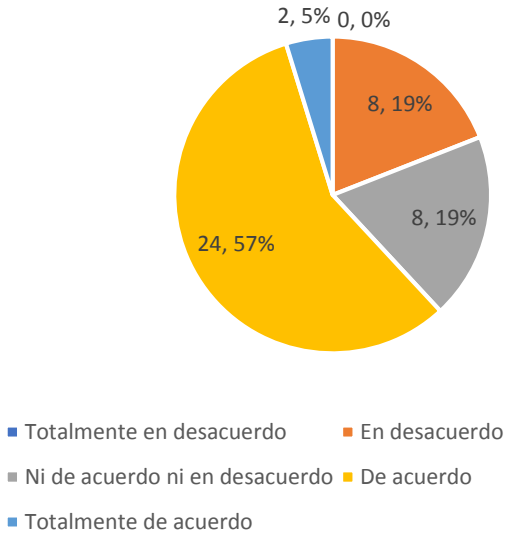
Cuadro de periodicidad de la magnitud ISO/IEC 27001.

Categorías	Frecuencia	Porcentaje (%)	Porcentaje acumulado
Totalmente en desacuerdo	0	0.0%	0.0%
En desacuerdo	8	19.0%	19.0%
Ni de acuerdo ni en desacuerdo	8	19.0%	38.1%
De acuerdo	24	57.1%	95.2%
Totalmente de acuerdo	2	4.8%	
Total	42	100%	

Nota: Dicho esquema es elaboración de mi autoría.

Figura 2

Ilustración de la magnitud ISO/IEC 27001



Nota: La presente representación es elaboración de mi autoría.

Interpretación: Como se puede visualizar en el cuadro 5 y en la representación 2, en lo que respecta a preguntas relacionadas a la

magnitud ISO/IEC 27001, predomina la categoría De acuerdo, con un 57.1%.

C) MAGNITUD 3: Administración de seguridad de la información

Tabla 6

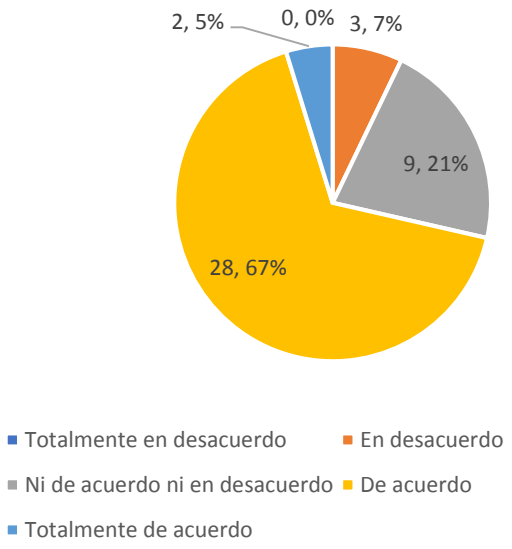
Cuadro de periodicidad de la magnitud Administración de seguridad de la información.

Categorías	Frecuencia	Porcentaje (%)	Porcentaje acumulado
Totalmente en desacuerdo	0	0.0%	0.0%
En desacuerdo	3	7.1%	7.1%
Ni de acuerdo ni en desacuerdo	9	21.4%	28.6%
De acuerdo	28	66.7%	95.2%
Totalmente de acuerdo	2	4.8%	
Total	42	100%	

Nota: Dicho esquema es elaboración de mi autoría.

Figura 3

Ilustración de la magnitud gestión de seguridad de la información.



Nota: La presente representación es elaboración de mi autoría.

Interpretación: Como se puede enfocar en el cuadro 6 y en la representación 3, En las cuestiones relacionadas con el grado de gestión de la seguridad de la información, la categoría de acuerdo dominó con un 66,7%.

D) MAGNITUD 4: SGSI.

TABLA 7

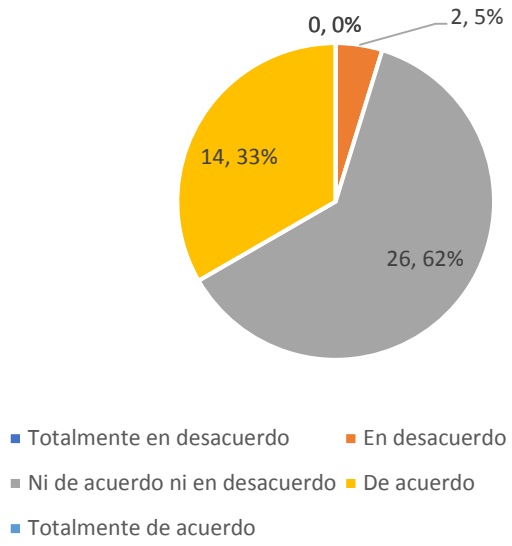
Cuadro de periodicidad de la magnitud SGSI.

Categorías	Frecuencia	Porcentaje (%)	Porcentaje acumulado
Totalmente en desacuerdo	0	0.0%	0.0%
En desacuerdo	2	4.8%	4.8%
Ni de acuerdo ni en desacuerdo	26	61.9%	66.7%
De acuerdo	14	33.3%	100.0%
Totalmente de acuerdo	0	0.0%	
Total	42	100%	

Nota: Dicho esquema es elaboración de mi autoría.

Figura 4

Ilustración de la magnitud Sistema gestión de seguridad de la información.



Nota: La presente representación es elaboración de mi autoría.

Interpretación: Como se puede visualizar en el cuadro 7 y en la representación 4, En las preguntas relacionadas con el tamaño de SGSI, prevaleció la categoría "Ni de acuerdo" o "en desacuerdo" con un 61,9%.

4.1.2. Explicación estadística: Variable calidad del servicio.

A) MAGNITUD 1: Perceptibles

TABLA 8

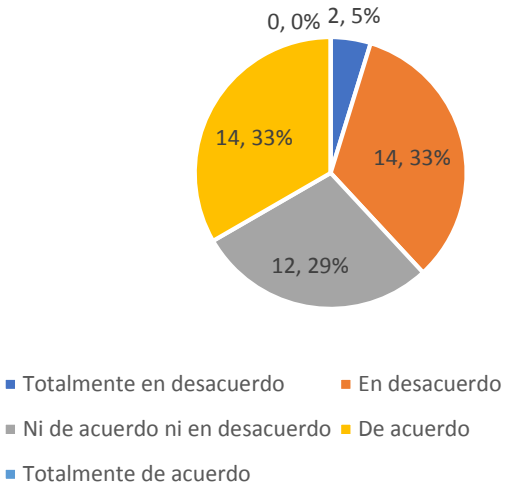
Cuadro de periodicidad de la magnitud perceptibles.

Categorías	Frecuencia	Porcentaje (%)	Porcentaje acumulado
Totalmente en desacuerdo	2	4.8%	4.8%
En desacuerdo	14	33.3%	38.1%
Ni de acuerdo ni en desacuerdo	12	28.6%	66.7%
De acuerdo	14	33.3%	100.0%
Totalmente de acuerdo	0	0.0%	
Total	42	100%	

Nota: Dicho esquema es elaboración de mi autoría.

Figura 5

Ilustración de la magnitud Perceptibles.



Nota: La presente representación es elaboración de mi autoría.

Interpretación: Como se puede visualizar en el cuadro 8 y en la representación 5, En las preguntas relacionadas con el tamaño percibido, las categorías dominantes fueron en desacuerdo y de acuerdo con un 33,3%.

B) MAGNITUD 2: Facultad de solución

TABLA 9

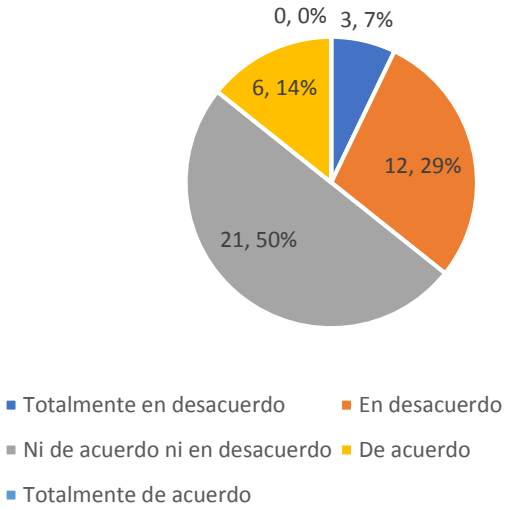
Cuadro de periodicidad de la magnitud facultad de solución

Categorías	Frecuencia	Porcentaje (%)	Porcentaje acumulado
Totalmente en desacuerdo	3	7.1%	7.1%
En desacuerdo	12	28.6%	35.7%
Ni de acuerdo ni en desacuerdo	21	50.0%	85.7%
De acuerdo	6	14.3%	100.0%
Totalmente de acuerdo	0	0.0%	
Total	42	100%	

Nota: Dicho esquema es elaboración de mi autoría.

Figura 6

Ilustración de la magnitud Facultad de solución.



Nota: La presente representación es elaboración de mi autoría.

Interpretación: Como se puede visualizar en el cuadro 9 y en la representación 6, En cuestiones relacionadas con la solidez de la solución, prevaleció la categoría "Ni de acuerdo" o "en desacuerdo" con un 50,0%.

C) MAGNITUD 3: Empatía

TABLA 10

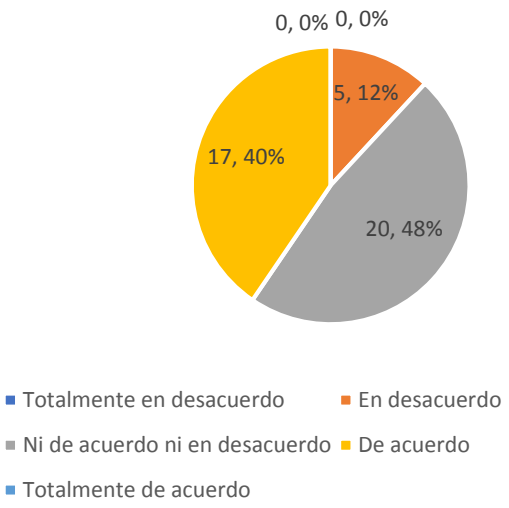
Cuadro de periodicidad de la magnitud empatía

Categorías	Frecuencia	Porcentaje (%)	Porcentaje acumulado
Totalmente en desacuerdo	0	0.0%	0.0%
En desacuerdo	5	11.9%	11.9%
Ni de acuerdo ni en desacuerdo	20	47.6%	59.5%
De acuerdo	17	40.5%	100.0%
Totalmente de acuerdo	0	0.0%	
Total	42	100%	

Nota: Dicho esquema es elaboración de mi autoría.

Figura 7

Ilustración de la magnitud empatía.



Nota: La presente representación es elaboración de mi autoría.

Interpretación: Como se puede visualizar en el cuadro 10 y en la representación 7, En cuanto a las preguntas relacionadas con el nivel de empatía, la mayoría se encontraba en las categorías "Ni de acuerdo" o "en desacuerdo", representando el 47,6%.

MAGNITUD 4: Seguridad

TABLA 11

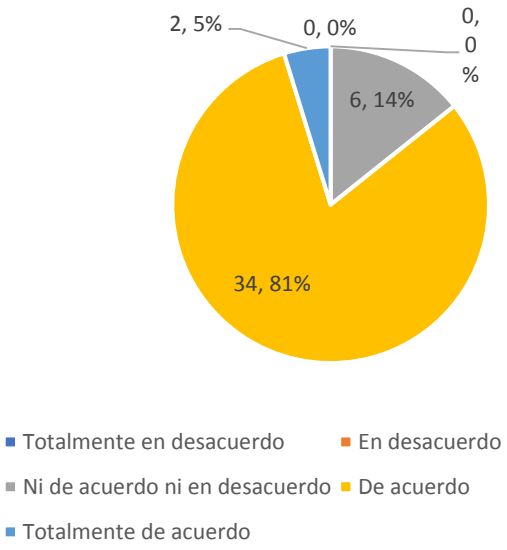
Cuadro de periodicidad de la magnitud seguridad

Categorías	Frecuencia	Porcentaje (%)	Porcentaje acumulado
Totalmente en desacuerdo	0	0.0%	0.0%
En desacuerdo	0	0.0%	0.0%
Ni de acuerdo ni en desacuerdo	6	14.3%	14.3%
De acuerdo	34	81.0%	95.2%
Totalmente de acuerdo	2	4.8%	
Total	42	100%	

Nota: Dicho esquema es elaboración de mi autoría.

Figura 8

Ilustración de la magnitud seguridad.



Nota: La presente representación es elaboración de mi autoría.

Interpretación: Como se puede visualizar en el cuadro 11 y en la representación 8, En cuestiones relacionadas con el nivel de seguridad, la categoría de acuerdo dominó con un 81,0%.

D) MAGNITUD 5: Fiabilidad

TABLA 12

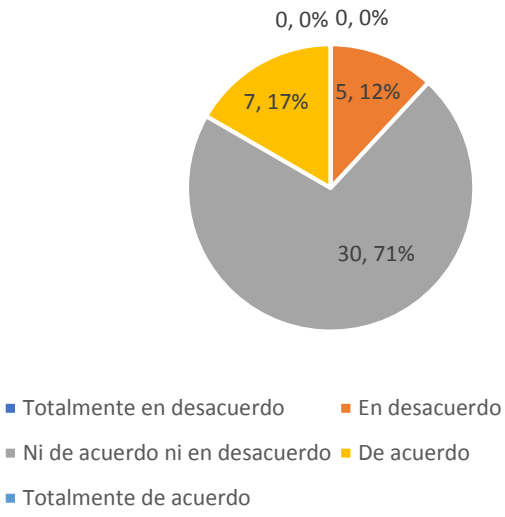
Cuadro de periodicidad de la magnitud fiabilidad.

Categorías	Frecuencia	Porcentaje (%)	Porcentaje acumulado
Totalmente en desacuerdo	0	0.0%	0.0%
En desacuerdo	5	11.9%	11.9%
Ni de acuerdo ni en desacuerdo	30	71.4%	83.3%
De acuerdo	7	16.7%	100.0%
Totalmente de acuerdo	0	0.0%	
Total	42	100%	

Nota: Dicho esquema es elaboración de mi autoría.

Figura 9

Ilustración de la magnitud fiabilidad.



Nota: La presente representación es elaboración de mi autoría.

Interpretación: Como se puede visualizar en el cuadro 12 y en la representación 9, en lo que respecta a preguntas relacionadas a la magnitud fiabilidad, prevaleció la categoría Ni de acuerdo ni en desacuerdo, con un 71.4%.

4.1.3. Resumen de las magnitudes de la variable: Sistema de gestión de seguridad de la información.

TABLA 13

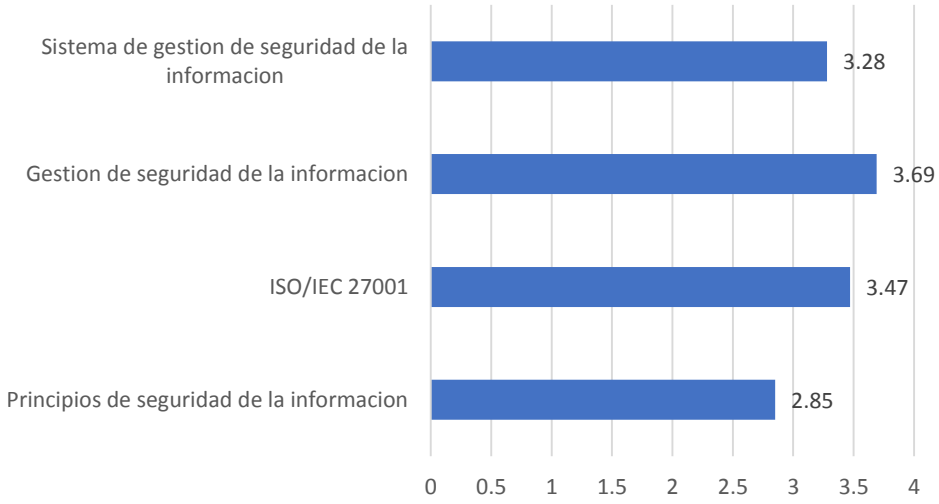
cuadro de Resumen de las magnitudes de la variable: Sistema de gestión de seguridad de la información.

Magnitudes	Media
Principios de seguridad de la información	2.85
ISO/IEC 27001	3.47
Administración de seguridad de la información	3.69
Sistema de gestión de seguridad de la información	3.28

Nota: Dicho esquema es elaboración de mi autoría.

Figura 10

Gráfica de Resumen de las magnitudes de la variable: Sistema de gestión de seguridad de la información



Acotación: Dicho esquema es elaboración de mi autoría.

Interpretación: Viendo en el cuadro 13 y en la representación 10, En cuanto a la variable sistema de gestión de seguridad de la información, domina el nivel de gestión de seguridad de la información con un valor medio de 3.69, seguido del nivel ISO/IEC 27001 con un valor medio de 3.47.

4.1.4. Resumen de las magnitudes de la variable: Calidad del servicio

TABLA 14

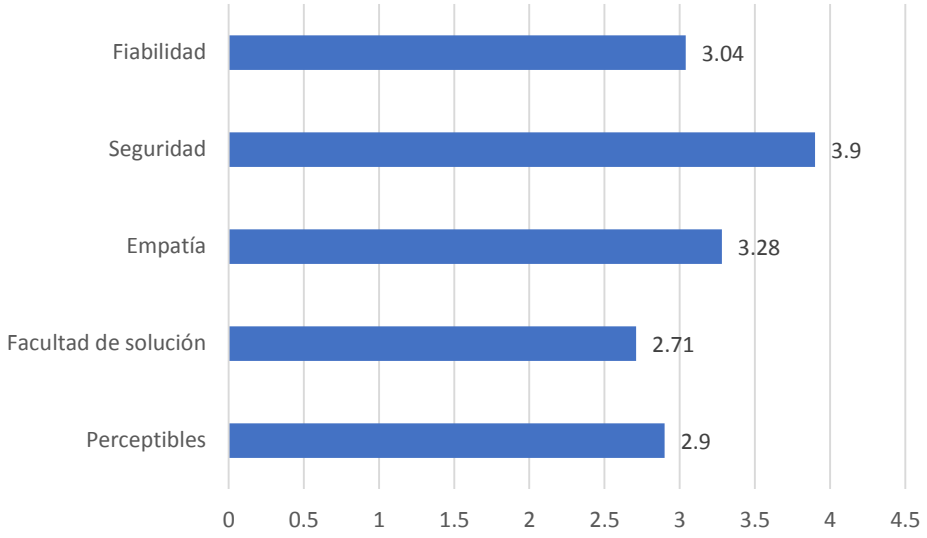
Cuadro de Resumen de las magnitudes de la variable: Calidad del servicio

Magnitud	Media
Perceptibles	2.9
Facultad de solución	2.71
Empatía	3.28
Seguridad	3.9
Fiabilidad	3.04

Nota: Dicho esquema es elaboración de mi autoría.

Figura 11

Gráfica de Resumen de las magnitudes de la variable: Calidad del servicio.



Acotación: Dicho esquema es elaboración de mi autoría.

Interpretación: Viendo en el cuadro 14 y en la representación 11, para la variable calidad del servicio, predomina la magnitud Seguridad, con una media de 3.9, seguido de la magnitud Empatía, con una media de 3.28.

4.2.Estadística inferencial de las variables

4.2.1. Contrastación con la hipotesis general.

H_1: Si existe una correlación relevante entre el SGSI y la calidad del servicio del colegio Carlos A. Velásquez Ilo.

H_0: No existe una correlación relevante entre el SGSI la calidad del servicio del colegio Carlos A. Velásquez Ilo.

TABLA 15

Cuadro de contingencia de las variables de estudio.

		Calidad del servicio					
	Categorías	Muy bajo	Bajo	Medio	Alto	Muy alto	Total
Sistema de gestión de seguridad de la información	Muy bajo	0	0	0	0	0	0
		0.0%	0.0%	0.0%	0.0%	0.0%	0.0%
	Bajo	0	2	0	0	0	2
		0.0%	4.8%	0.0%	0.0%	0.0%	4.8%
	Medio	0	1	18	7	0	26
		0.0%	2.2%	41.7%	18.0%	0.0%	61.9%
	Alto	0	0	2	12	0	14
		0.0%	0.0%	4.5%	28.9%	0.0%	33.3%
	Muy alto	0	0	0	0	0	0
		0.0%	0.0%	0.0%	0.0%	0.0%	0.0%
	Total	0	3	20	19	0	42
		0.0%	7.0%	46.2%	46.9%	0.0%	100%
	Prueba Chi-cuadrado			40.11 GL=4			

Nota: Dicho esquema es elaboración de mi autoría.

Como puede notarse en el cuadro 15, Tenemos un valor de chi-cuadrado calculado de x^2 = 40,11, que es mayor que x^2 cuadro = 9,40; por lo tanto, frente a la hipótesis nula H0, aceptamos la hipótesis alternativa H1, que muestra que el SGSI está estrechamente relacionado con la calidad del servicio.

Grado de correlación

TABLA 16

Nivel de correlación entre el sistema de gestión de la seguridad de la información y calidad del servicio.

Coeficiente de correlación de Spearman (r_s)	Calidad del servicio
Sistema de gestión de la seguridad de la información	$r_s = 0.58$
Valor -p	0.00

Nota: Dicho esquema es elaboración de mi autoría.

Como vemos en el cuadro 16, El nivel de correlación entre el SGSI y las variables de calidad del servicio es de 0,58. Según la tabla de interpretación de Bisquerra se encuentra en la categoría media, por lo que existe una relación positiva promedio, si el valor de una variable aumenta, el valor de la otra variable también aumenta. Por tanto, considerando que el valor de p=0,00 está por debajo del nivel de significación elegido (α=0,05), se confirma la existencia de una correlación estadísticamente significativa entre las variables de estudio.

4.2.2. Contrastación de primera hipótesis específica

H_1: Los principios de seguridad de información se correlacionan en gran medida con la calidad del servicio del colegio Carlos A. Velásquez Ilo.

H_0: Los principios de seguridad de información no se correlacionan en gran medida con la calidad del servicio del colegio Carlos A. Velásquez Ilo.

TABLA 17

Cuadro de contingencia de principios de seguridad de la información contra calidad del servicio.

		Calidad del servicio					
	Categorías	Muy bajo	Bajo	Medio	Alto	Muy alto	Total
Principios de seguridad de la información	Muy bajo	0	0	1	0	0	1
		0.0%	0.0%	2.3%	0.0%	0.0%	2.3%
	Bajo	0	2	10	0	0	12
		0.0%	4.6%	23.9%	0.0%	0.0%	28.5%
	Medio	0	1	14	6	0	21
		0.0%	2.2%	33.7%	14.1%	0.0%	50.0%
	Alto	0	0	1	7	0	8
		0.0%	0.0%	2.2%	16.9%	0.0%	19.1%
	Muy alto	0	0	0	0	0	0
		0.0%	0.0%	0.0%	0.0%	0.0%	0.0%
	Total	0	3	26	13	0	42
		0.0%	6.8%	62.1%	31.0%	0.0%	100%
	Prueba Chi-cuadrado			12.98 GL=6			

Nota: Dicho esquema es elaboración de mi autoría.

Como puede notarse en el cuadro 17, se tiene un valor de Chi-cuadrado $x^2_{calculado} = 12.98$, el cual es mayor que $x^2_{tabla} = 12.57$; Por lo tanto, se contrapone la hipótesis nula H0 y se acepta la hipótesis alternativa H1, lo que demuestra que los principios de seguridad de la información y la calidad del servicio están estrechamente relacionados.

Grado de correlación

TABLA 18

Nivel de correlación entre principios de seguridad de la información y calidad del servicio

Coeficiente de correlación de Spearman (r_s)	Calidad del servicio
Principios de seguridad de la información	$r_s = 0.35$
Valor -p	0.01

Nota: Dicho esquema es elaboración de mi autoría.

Como vemos en el cuadro 18, El nivel de correlación entre tamaño y variables de investigación, principios de seguridad de la información y calidad del servicio es de 0,35. Según el cuadro explicativo de Bisquerra, por tanto, existe una menor correlación positiva, y a medida que aumenta la magnitud del principio también lo hace el valor de la variable calidad del servicio. Considerando que el valor de p=0,01 es inferior al nivel de significancia elegido (α=0,05), se confirma una relación estadísticamente significativa entre el tamaño y las variables estudiadas.

4.2.3. Contrastación de segunda hipótesis específica

H_1: El ISO/IEC 27001 se correlaciona en gran medida con la calidad del servicio del colegio Carlos A. Velásquez Ilo.

H_0: El ISO/IEC 27001 no se correlaciona en gran medida con la calidad del servicio del colegio Carlos A. Velásquez Ilo.

TABLA 19

Cuadro de contingencia de ISO/IEC 27001 contra calidad del servicio.

		Calidad del servicio					
	Categorías	Muy bajo	Bajo	Medio	Alto	Muy alto	Total
ISO/IEC 27001	Muy bajo	0	0	0	0	0	0
		0.0%	0.0%	0.0%	0.0%	0.0%	0.0%
	Bajo	0	0	8	0	0	8
		0.0%	0.0%	19.0%	0.0%	0.0%	19.0%
	Medio	0	0	8	0	0	8
		0.0%	0.0%	19.0%	0.0%	0.0%	19.0%
	Alto	0	0	19	5	0	24
		0.0%	0.0%	42.2%	14.9%	0.0%	57.1%
	Muy alto	0	0	0	2	0	2

	0.0%	0.0%	0.0%	4.8%	0.0%	4.8%
Total	0	0	35	7	0	42
	0.0%	0.0%	80.2%	19.7%	0.0%	100%
Prueba			11.35			
Chi-cuadrado			GL=6			

Nota: Dicho esquema es elaboración de mi autoría.

Como puede notarse en el cuadro 19, se tiene un valor de Chi-cuadrado $x^2_{calculado} = 11.35$, el cual es menor que $x^2_{tabla} = 12.45$; por lo que se objeta la hipótesis nula H_1 y se acepta la hipótesis alterna H_0, la cual muestra la ISO/IEC 27001 no se correlaciona en gran medida con la calidad del servicio del colegio Carlos A. Velásquez Ilo

Grado de correlación

TABLA 20

Nivel de correlación entre ISO/IEC 27001 y calidad del servicio.

Coeficiente de correlación de Spearman (rs)	Calidad del servicio
ISO/IEC 27001	rs = 0.28
Valor -p	0.05

Nota: Dicho esquema es elaboración de mi autoría.

Como vemos en el cuadro 20, El nivel de correlación entre tamaño y variables de la encuesta, ISO/IEC 27001 y calidad del servicio es de 0,28. Por lo tanto, según la tabla de interpretación de Bisquerra, existe una relación moderadamente positiva en la categoría baja, y a medida que aumenta el tamaño de la ISO/IEC 27001, también aumenta el valor de la variable calidad del servicio. Sin embargo, se confirmó que no existe una relación estadísticamente significativa entre la magnitud y las variables en

estudio, dado que el valor de p=0,05 es mayor que el nivel de significancia elegido (α=0,05).

4.2.4. Contrastación de tercera hipótesis específica

H_1: La administración de seguridad de la información se correlaciona en gran medida con la calidad del servicio del colegio Carlos A. Velásquez Ilo.

H_0: La administración de seguridad de la información no se correlaciona en gran medida con la calidad del servicio del colegio Carlos A. Velásquez Ilo.

TABLA 21

Cuadro de contingencia de administración de seguridad de la información contra calidad del servicio.

		Calidad del servicio					
	Categorías	Muy bajo	Bajo	Medio	Alto	Muy alto	Total
Administración de seguridad de la información	Muy bajo	0	0	0	0	0	0
		0.0%	0.0%	0.0%	0.0%	0.0%	0.0%
	Bajo	0	1	2	0	0	3
		0.0%	2.2%	4.9%	0.0%	0.0%	7.1%
	Medio	0	0	7	2	0	9
		0.0%	0.0%	16.5%	4.9%	0.0%	21.4%
	Alto	0	0	22	6	0	28
		0.0%	0.0%	48.7%	18.0%	0.0%	66.7%
	Muy alto	0	0	0	2	0	2
		0.0%	0.0%	0.0%	4.8%	0.0%	4.8%
	Total	0	1	31	10	0	42
		0.0%	2.2%	70.1%	27.7%	0.0%	100%
	Prueba Chi-cuadrado			20.19 GL=6			

Nota: Dicho esquema es elaboración de mi autoría.

Como puede notarse en el cuadro 21, se tiene un valor de Chi-cuadrado $x^2_{calculado} = 20.19$, el cual es mayor que $x^2_{tabla} = 12.57$; por lo que se objeta la hipótesis nula H_0 y se toma la hipótesis alterna H_1, la cual muestra que la administración de seguridad de la información y la calidad del servicio se correlacionan en gran medida.

Nivel de correlación

TABLA 22

Nivel de correlación entre la administración de seguridad de la información y calidad del servicio.

Coeficiente de correlación de Spearman (rs)	Calidad del servicio
Administración de seguridad de la información	rs = 0.36
Valor -p	0.01

Nota: Dicho esquema es elaboración de mi autoría.

Como vemos en el cuadro 22, El nivel de correlación entre esta cantidad y las variables de investigación, gestión de la seguridad de la información y calidad del servicio es de 0,36. Según la tabla de interpretación de Bisquerra, que se encuentra en la categoría baja y por lo tanto tiene una correlación positiva menor, a medida que aumenta la cantidad de gestión de seguridad de la información también aumenta el valor de la variable calidad del servicio. Al estar el valor de p=0,01 por debajo del nivel de significancia elegido (α=0,05), se confirma una correlación estadísticamente significativa entre la magnitud y las variables estudiadas.

4.2.5. Comparación de cuarta hipótesis específica

H_1: El SGSI se correlaciona en gran medida con la calidad del servicio del colegio Carlos A. Velásquez Ilo.

H_0: El SGSI no se correlaciona en gran medida con la calidad del servicio del colegio Carlos A. Velásquez Ilo

TABLA 23

Cuadro de contingencia SGSI y calidad del servicio.

		Calidad del servicio					
	Categorías	Muy bajo	Bajo	Medio	Alto	Muy alto	Total
Sistema de gestión de seguridad de la información	Muy bajo	0	0	0	0	0	0
		0.0%	0.0%	0.0%	0.0%	0.0%	0.0%
	Bajo	0	0	2	0	0	2
		0.0%	0.0%	4.8%	0.0%	0.0%	4.8%
	Medio	0	0	20	6	0	26
		0.0%	0.0%	43.5%	18.4%	0.0%	61.9%
	Alto	0	1	12	1	0	14
		0.0%	2.2%	28.9%	2.2%	0.0%	33.3%
	Muy alto	0	0	0	0	0	0
		0.0%	0.0%	0.0%	0.0%	0.0%	0.0%
	Total	0	1	34	7	0	42
		0.0%	2.2%	77.2%	20.6%	0.0%	100%
	Prueba Chi-cuadrado			10.49 GL=4			

Nota: Dicho esquema es elaboración de mi autoría.

Como puede notarse en el cuadro 23, se tiene un valor de Chi-cuadrado $x^2_{calculado} = 10.49$, el cual es mayor que $x^2_{tabla} = 9.40$; por lo que se objeta la hipótesis nula H_0 y se toma la hipótesis alterna H_1, la cual muestra que el sistema de gestión de seguridad de la información y la calidad del servicio se correlacionan en gran medida.

Grado de correlación

TABLA 24

Nivel de correlación entre el sistema de gestión de seguridad de la información y calidad del servicio.

Coeficiente de correlación de Spearman (rs)	Calidad del servicio
Sistema de gestión de seguridad de la información	rs = 0.43
Valor -p	0.002

Nota: Dicho esquema es elaboración de mi autoría.

Como vemos en el cuadro 24, el nivel de correlación es de 0.43 La relación entre tamaño y variables de encuesta, SGSI y calidad del servicio. Por lo tanto, según la tabla de interpretación de Bisquerra, al estar en la categoría media, si hay una correlación positiva, se pasa a la categoría media, y a medida que aumenta el tamaño del SGSI, también aumenta el valor de la variable calidad del servicio. Al estar el valor de p=0,02 por debajo del nivel de significancia elegido (α=0,05), se confirma una correlación estadísticamente significativa entre la magnitud y las variables estudiadas.

4.3.Discusión de resultados.

El principal objetivo del estudio es proponer al Colegio Carlos A. Velásquez Ilo un sistema de gestión de seguridad de la información que utilice la norma ISO 27001 para reducir el riesgo de pérdida de información. Para ello se evaluó la situación existente del colegio y se precisaron los requisitos para la protección de los activos, que eran información en ausencia de activos, las mejoras reflejan los tres pilares del mantenimiento de activos: confidencialidad, disponibilidad

e integridad. También es necesario encuestar a los profesores administrativos para comprender sus percepciones.

Interpretación: Como se puede deducir en el cuadro 13 y representación 10, para la variable de, SGSI domina la magnitud administración de S.I, con una media de 3.69. seguido de la magnitud ISO 3.47.

CAPÍTULO V:

CONCLUSIONES Y RECOMENDACIONES

1.1.Conclusiones

Primera conclusión, se verifico que, si existe una coherencia entre las variables de SGSI y la calidad del servicio, accediendo a plantear los problemas de seguridad en la información, todo esto para mejorar sus procesos de la mano con la normativa ISO 27001, lo cual mejorará en minimizar la perdida de información. Así mismo se observó que el personal tenía poco conocimiento en cuanto ciberseguridad.

Segunda Conclusión, al identificar los principios de S.I. en correlación a la calidad del servicio del colegio Carlos A. Velásquez Ilo fue implantar orientaciones en la S.I de los sistemas que maneja el colegio.

Tercera conclusión, al identificar la normativa ISO/IEC 27001 en correlación a la calidad del servicio del colegio Carlos A. Velásquez Ilo fue implantar normativas de desempeño en los controles de seguridad para la verificación del nivel de seguridad cumpliendo y reduciendo los riesgos ante perdidas, sabotajes y fraudes de información dando una satisfacción de mejora en los sistemas del colegio.

Cuarta conclusión, al determinar la correlación entre el SGSI y la calidad del servicio del colegio Carlos A. Velásquez Ilo fue importante determinar dicha correlación y evaluar el estado actual de los procesos de seguridad utilizados en las computadoras mientras se consideran los estándares de gestión de la información para mejorar los procesos.

1.2.Recomendaciones

1. Hacer de conocimiento al director y equipo directivo, la importancia de la integración de las TIC que el personal docente administrativo del colegio Carlos A. Velásquez Ilo debe conocer, así mismo manifestar que sean capacitados periódicamente en lo que es alfabetización digital, herramientas TIC, ciberseguridad, entre otras tanto por el personal a cargo o solicitando a las diferentes entidades como la UGEL Ilo, Minedu, gobierno regional.
2. En todo ese periodo de conocimiento, adaptabilidad y actualización utilizando las normas ISO, evaluar la seguridad de la información según cronogramas establecidos para garantizar que se apliquen los procesos preventivos que ayuden a la mejora y continuidad de los servicios.
3. Puesto que actualmente no se cuenta con un aula y/o área dedicada al control y seguridad de la información, se propone al director y equipo directivo plantear estratégicamente la elaboración de un área dedicado a la administración de tecnologías, entre ellos, en relación con los cambios en la I.E. Carlos A. Velásquez Ilo, es necesario adaptar nuevos requisitos de seguridad, y que haya un responsable en dicha área.
4. Proponer la elaboración de un proyecto donde la administración pueda certificarse con la Norma ISO/IEC 27001, para que toda mejora pueda adaptarse con los lineamientos establecidos y así el colegio Carlos A. Velásquez Ilo sea modelo a seguir por otras instituciones educativas.

REFERENCIAS BIBLIOGRÁFICAS

Acosta-Ramírez, H. (2017). *Diseño de un plan de contingencia del sistema de información para la entidad ITRC* [Tesis de pregrado, Universidad Nacional Abierta y a distancia UNAD]. Repositorio Unad. https://repository.unad.edu.co/bitstream/handle/10596/13868/19306734.pdf?sequence=1

Aguilera, P. (2010). *Seguridad informática*. Editex, S.A.

Alemán-Novoa, H. y Rodríguez-Barrera C. (2014). Metodologías Para el Análisis de Riesgos en los SGSI. *Revista especializada en ingeniería, 9* (2015), 1-14

Arroyo Fuentes, A. (2016). *Conocimiento digital*. https://grupo4herramientasinformatica.blogspot.pe/2016/03/la-seguridad-informatica.html.

Barrantes, C. y Hugo. J. (2012). *Diseño e implementación de un sistema de gestión de seguridad de información en procesos tecnológicos* [Tesis de pregrado, Universidad San Martin de Porres]. Repositorio digital USMP. https://repositorio.usmp.edu.pe/bitstream/handle/20.500.12727/609/barrantes_ce.pdf?sequence=3&isAllowed=y

Bernal, C. (2013). *Metodología de la investigación. 3º edición.* D.R. ©2010 por Pearson Educación de Colombia Ltda. https://abacoenred.com/wp-content/uploads/2019/02/El-proyecto-de-investigaci%C3%B3n-F.G.-Arias-2012-pdf.pdf

Calderón-Romero, V. (2017). *Plan de contingencia para el departamento de sistemas de la empresa Ramón & Romero computadoras y suministros de la ciudad de Quevedo* [Tesis de pregrado, Universidad Regional Autónoma

de los Andes]. Repositorio institucional UNIANDES. https://dspace.uniandes.edu.ec/handle/123456789/7523

Campoy, T., y Gómez, E. (2015). *Procedimientos y mecanismos cualitativos de recogida de datos*. Universidad de la Costa. https://upla.edu.pe/wp-content/uploads/2017/12/2-UPLA- Instrumentos-cualitativos-de-datos.pdf

Carrasco-Ramírez, F. (2015). *Desarrollo e implantación de un plan de contingencia informática para la dirección de tecnologías de la información de la pontificia universidad católica del Ecuador sede Santo Domingo* [Tesis de maestría, Escuela Superior Politécnica del Litoral]. Repositorio Dspace. http://www.dspace.espol.edu.ec/xmlui/handle/123456789/30022?show=full

Castro, M. (2003). *El proyecto de investigación y su esquema de elaboración*. *2º edición.* Caracas: Uyapal.

Castro-Quinde, C. (2014). *Elaboración de un sistema de gestión de seguridad de la información (SGSI) para la empresa radical Cia. Ltda. en la ciudad de Quito para el año 2014* [Tesis de maestría, Universidad de las Américas]. Repositorio Digital Universidad De Las Américas. https://dspace.udla.edu.ec/handle/33000/3376

Corrales, J. (2005). *Ayudante Técnicos. Opción Informática. Junta de Andalucía*. España: MAD, S.L.

Chicano, E. (2014). *Gestión de Incidentes de Seguridad Informática*. IFCT0109. Málaga: IC Editorial.

Deming, W. (1986). *The Deming Management Method*. Nota. https://smallbusiness.chron.com/deming-management-method-74172.html

Disterer, G. (2013). ISO/IEC 27001 para la gestión de la seguridad de la información. *Revista de Seguridad de la Información, 4*, 92-100. http://dx.doi.org/10.4236/jis.2013.42011

Erb, M. (2005). *Gestión de Riesgo en la Seguridad Informática*. https://protejete.wordpress.com/gdr_principal/seguridad_informacion_proteccion

Estándares, O. I. (s.f.). ISO 27000. WWW.ISO27000.ES.

Fernández, C. (2012). *La Norma ISO 27001 del Sistema de Gestión de Seguridad de Información, garantía de confidencialidad, Integridad y disponibilidad.* España: Asociación Española de Normalización y Certificación.

Fontalvo, T., Vergara, J., & de la Hoz, E. (2012). Evaluación del impacto de los sistemas de gestión de la calidad en la liquidez y rentabilidad de las empresas de la zona industrial Vía 40. *Pensamiento & gestión, 32*. Universidad del Norte, 165-189, 2012.

García, A., Hurtado, C., Alegre, M. (2011). *Seguridad informática*. Paraninfo, S.A.

Godoy, R. (2014). *Seguridad de Información*. Guatemala: Revista de la Segunda Cohorte del Doctorado en Seguridad Estratégica.

Gómez A., (2011). *Enciclopedia de la seguridad informática 2º edición*. Ra-Ma S.A. Editorial y Publicaciones, 2011.

Gonzales, H., y Delgado, I. (2018). *Diseño del plan de contingencia como herramienta para gestionar riesgos de la seguridad de la información en el área del centro de sistemas de información de la ugel-ferreñafe en el periodo 2018* [Tesis de pregrado, Universidad de Lambayeque]. Repositorio Dspace. https://repositorio.udl.edu.pe/xmlui/handle/UDL/235

Hernández, R. (2014). *Metodología de la investigación. Mc Graw Hill Education 6a edición*. http://observatorio.epacartagena.gov.co/wp-content/uploads/2017/08/metodologia-de-la-investigacion-sexta-edicion.compressed.pdf

INEI (2006). *Órgano Rector de los Sistemas Nacionales de Estadística e Informática Perú*. Editorial Instituto Nacional de Estadística e Informática.

ISO/IEC. (2014). ISO/IEC 27000 Tecnología de datos - Técnicas de protección - Sistemas de administración de protección de la información ISO/IEC.

ISO/IEC 27000:2016. Tecnología de la información -Técnicas de seguridad - Sistemas de gestión de la seguridad de la información - Visión general y vocabulario.

Juran, J. (1989). *Juran on Planning for Quality. ASQ*. https://doi.org/10.1007/s00217-011-1549-y

Kotler y Armstrong (2013). *Definición de marketing y del proceso de marketing*. D.R. © 2013 por Pearson Educación de México, S.A. de C.V. https://frrq.cvg.utn.edu.ar/pluginfile.php/14584/mod_resource/content/1/Fundamentos%20del%20Marketing-Kotler.pdf

Ladines-Garcés, K. (2017). *Plan informático de contingencia para la seguridad de la información del departamento de TIC de la Pucese* [Tesis de pregrado, Pontificia Universidad Católica del Ecuador sede Esmeraldas]. Repositorio Digital PUCESE. https://repositorio.pucese.edu.ec/handle/123456789/1010

León, D. (2007). Plan de contingencia para el archivo de la universidad de la Salle como parte de la implantación del sistema integrado de conservación. *Revista Códice*, *4*(1), 1-6.

López, P. (2004). Población Muestra y Muestreo. *Revista Punto Cero, 9*(0), 1-6.

(López, 2004). Población muestra y muestreo. *Punto Cero v.09* (08). Cochabamba 2004. http://www.scielo.org.bo/scielo.php?script=sci_arttext&pid=S1815-02762004000100012

Mero-Suárez, C. (2018). *Plan de contingencias informáticas y la seguridad de la información en el consejo nacional electoral de la provincia de santa elena* [Tesis de maestría, Universidad regional autónoma de los andes]. Repositorio institucional UNIANDES. https://dspace.uniandes.edu.ec/bitstream/123456789/9060/1/TUAEXCOMMIE004-2018.pdf

Mujica, M. y Álvarez, Y. (2011). Análisis y gestión de riesgos de seguridad de la información. *Revista en ciencias y tecnologías, 4*(2), 1-6.

Moscaiza-Moncada, O. (2018). *Diseño de un sistema de gestión de la seguridad de la información (SGSI) para la cooperativa de ahorro y crédito ABC, basado en la norma ISO 27001:2013* [Tesis de pregrado, Universidad peruana de ciencias aplicadas]. Repositorio académico UPC. https://repositorioacademico.upc.edu.pe/handle/10757/623063

Myler, E. y Broadbent, G. (2006). ISO 17799: Standard for Security. *Information Management Journal, 40*(6), 43-44,46,48-52.

Norma ISO 27001 (Organización Internacional de Estándares). (2013*). Sistema de Gestión de Seguridad de Información (SGSI)*. www.ISO27000.ES.

Rodríguez, G., Gil, J., & García, E. (1996). *Metodología de la investigación cualitativa*. Ediciones Aljibe. Granada (España). 1996.

Seclén-Arana, J. (2016). *Factores que afectan la implementación del sistema de gestión de seguridad de la información en las entidades públicas peruanas de acuerdo a la NTP-ISO/IEC 27001* [Tesis de maestría, Universidad Nacional Mayor de San Marcos]. Repositorio de tesis digitales CYBERTESIS. https://hdl.handle.net/20.500.12672/4884

Tarrillo, E. y Correa. J. (2015). *Metodología para un sistema de gestión de la seguridad de la información basado en la norma técnica peruana NTP-17799 en la administración de la municipalidad distrital de Lambayeque setiembre 2013- febrero 2014* [Tesis de pregrado, Universidad Nacional Pedro Ruiz Gallo]. Repositorio Institucional UNPRG. https://repositorio.unprg.edu.pe/handle/20.500.12893/499

Terán D. (2014). *Administración Estratégica de la Función Informática*. México: Alfaomega.

Torres, M. y Paz, K. (2006). Métodos de recolección de datos, para una investigación. *Facultad de Ingeniería - Universidad Rafael Landívar, Boletín*, (03), 1-21.

Verdú-Fernández, J. (2015). *Plan de contingencia de tecnologías de la información en entornos distribuidos* [Tesis de pregrado, Universidad Carlos III de Madrid]. Repositorio digital. https://e-archivo.uc3m.es/bitstream/handle/10016/22424/PFC_Jose_Ignacio_Verdu_Fernandez.pdf?sequence=1&isAllowed=y

Vergara-Quiroz, G. (2016). *Seguridad de información y calidad de servicio en la universidad nacional federico Villarreal, 2016* [Tesis de maestría,

Universidad Cesar Vallejo]. Repositorio de la universidad Cesar Vallejo. https://repositorio.ucv.edu.pe/handle/20.500.12692/22150

Yan, f., y Zavala, C. (2018). *Plan de mejora de la seguridad de la información y continuidad del centro de datos de la gerencia regional de educación de la libertad aplicando lineamientos ISO 27001 y buenas prácticas cobit* [Tesis de pregrado, Universidad privada Antenor Orrego]. Repositorio digital de la Universidad Privada Antenor Orrego. https://repositorio.upao.edu.pe/handle/20.500.12759/645

ANEXO 1

TABLA 25

ANEXO 1: MATRIZ DE CONSISTENCIA

PROBLEMA	OBJETIVOS	HIPÓTESIS	VARIABLES E INDICADORES		
1. GENERAL	**1. GENERAL**	**1. GENERAL**	**1. Variable Independiente**		
			Sistema de Gestión de seguridad de la Información		
¿Entre el sistema de gestión de seguridad de la información y la calidad del servicio del colegio Carlos A. Velásquez Ilo, cuál sería su correlación?	Establecer cuál será la correlación entre un sistema de gestión de seguridad de información y la calidad del servicio del colegio Carlos A. Velásquez Ilo.	Si existe una correlación entre el sistema de gestión de seguridad de la información y la calidad del servicio del colegio Carlos A. Velásquez Ilo	**1.1 Operacionalización**		
			DIMENSIONES	**INDICADORES**	**INDICE**
2. ESPECÍFICOS	**2. ESPECÍFICOS**	**2. ESPECÍFICOS**		Disponibilidad	
			Principios de seguridad de la información. (Standar, 2005)	Confidencialidad	
¿Cuáles serán los principios de seguridad de la información en correlación a la calidad del Servicio del colegio Carlos A. Velásquez Ilo?	Identificar los principios de seguridad de la información en correlación a la calidad del servicio del colegio Carlos A. Velásquez Ilo	Los inicios de protección de la información; se correlacionan en gran medida con la calidad del servicio del colegio Carlos A. Velásquez Ilo.		Integridad	Si / No **Ordinal**
				Normas de la seguridad de la información	
			Norma ISO/IEC 27001 (ISO 2015)	Conocimiento	
				Capacitación	

¿Cómo el ISO/IEC 27001 se correlaciona con la calidad del servicio del colegio Carlos A. Velásquez Ilo?	Identificar como el ISO/IEC27001 se correlaciona con la calidad del servicio del colegio Carlos A. Velásquez Ilo.	El ISO/IEC 27001. Se correlaciona en gran medida con la calidad del servicio de colegio Carlos A. Velásquez Ilo.	Administración de sistema de gestión de seguridad de la información (Disterer, G., 2013)	Existencia de Personal y métodos de divulgación Sistema de gestión de seguridad Medición de seguridad
¿Cómo la administración de seguridad de la información se correlaciona con la calidad del servicio del colegio Carlos A. Velásquez Ilo?	Identificar la administración de seguridad de la información en correlación con la calidad del servicio del colegio Carlos A. Velásquez Ilo.	La administración de seguridad de la información; se correlaciona en gran medida con la calidad del servicio del colegio Carlos A. Velásquez Ilo		Personal especializado Medios de respaldo para recuperar información. Monitoreo y evaluación de procesos de contingencia y restauración Comunicación inmediata ante siniestros presentados
¿Cómo el sistema de gestión de seguridad de la información se correlaciona con la calidad del Servicio del colegio Caros A. Velásquez Ilo?	Identificar como el sistema de gestión de seguridad de la información se correlaciona con la calidad del servicio del Colegio Carlos A. Velásquez Ilo.	El Sistema de gestión de seguridad de la información. Se correlaciona en gran medida con la calidad del servicio del colegio Carlos A. Velásquez Ilo.	Sistema de gestión de seguridad de la información (ISO 2015)	Políticas de seguridad Gestión de riesgos Auditorias Elaboración documentada Actualización y mejoras

2. Variable dependiente

Calidad del servicio del colegio Carlos A. Velásquez Ilo

Operacionalización

DIMENSIONES	INDICADORES	INDICE
Perceptibles	Identificación Apariencia Tecnología Aspecto Profesionalismo	**Ordinal** 1. Totalmente en desacuerdo 2. En desacuerdo
Facultad de solución	Tiempos Acceso Flexibilidad eficiente	3. Ni de acuerdo ni en desacuerdo
Empatía	Disponibilidad Respetuoso Servicial habilidad	4. De acuerdo
Seguridad	Credibilidad Oportuno	5. Totalmente de acuerdo
Fiabilidad	Confianza	

TIPO Y DISEÑO	POBLACIÓN Y MUESTRA	TÉCNICAS E INSTRUMENTOS	ESTADÍSTICA DESCRIPTIVA E INFERENCIAL
TIPO DE ESTUDIO	**POBLACION**	**VARIABLE INDEPENDIENTE**	
a) Descriptivo, evalúa, mide y dimensiones del fenómeno a estudiar con el fin de describir cómo se presenta el problema de investigación. Nos ofrece información para la realización de investigaciones posteriores y para abarcar estrategias adecuadas de enfrentarse a ellas. b) Correlacional, porque evalúa el nivel de relación/correlación entre dos variables a estudiar	La población está conformada por 35 miembros que utilizan los sistemas informáticos del colegio Carlos A Velásquez Ilo	Sistema de gestión de la seguridad de la información - Técnica: utilizamos encuesta - Instrumentos: Cuestionario - Tipo de escala: Ordinal - Confiabilidad: Coeficiente de Alfa de Cronbach - Ámbito de aplicación: Colegio Carlos A. Velásquez - Forma de administración: Encuesta directa	Estadística descriptiva para representar tablas de contingencia y figuras
DISEÑO DE INVESTIGACION	**MUESTRA**		
No experimental, las variables no se variarán intencionalmente y de corte transversal/transeccional porque se efectuará en	En la presente investigación emplearemos el total de la población por lo que no		En estadística, el coeficiente de Correlación de Spearman, p, es una medida de la correlación entre dos variables aleatorias continuas. Para calcular "p",

un único momento (Hernández, 2014): a) Diseño no experimental, debido a que los elementos causales no se manipulan para determinar sus efectos posteriormente. Para describir y analizar la incidencia o interrelación en un momento dado por las variables b) Transversal, incluyendo el nivel descriptivo-correlacional para su estudio.	necesita una muestra	**VARIABLE DEPENDIENTE** Calidad del servicio del colegio Carlos A. Velásquez Ilo - Técnica: Encuesta - Instrumentos: Cuestionario - Tipo de escala: Ordinal - Confiabilidad: Coeficiente de Alfa de Cronbach - Ámbito de aplicación: Colegio Carlos A. Velásquez - Forma de administración: Encuesta directa	Los datos se clasifican y reemplazan en el orden correcto. $$p = 1 - \frac{6 \sum d\text{^}2}{n(n\text{^}2 - 1)}$$ Donde: p= Coeficiente de correlación por rangos de Spearman ∑ = Diferencia entre los rangos d = Diferencia entre los correspondientes estadísticos n = Número de parejas Nivel de significación si p < 0.05 => existe relación entre las variables

Nota: Elaboración propia